Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

| | | |
|---|---|---|
| In the Matter of: | ) | |
| | ) | |
| Digital Broadcast Copy Protection | ) | MB Docket No. 02-230 |

COMMENTS OF THE INFORMATION TECHNOLOGY INDUSTRY COUNCIL

The Information Technology Industry Council ("ITI") hereby submits its comments in response to the Notice of Proposed Rulemaking released in the above-referenced proceeding. ITI represents the leading US providers of information technology products and services. ITI members have aggregate annual revenues in excess of $661 billion and directly employ more than one million people in the United States.

The information technology ("IT") industry has a long history of combating digital piracy of its own products, responding to more than $11 billion annually in software piracy - and of workig to protect digital entertainment content, investing hundreds of millions of dollars in new digital rights management technologies to securely deliver digital entertainment content as well as generally private and sensitive personal information. In our view, a serious effort to fight piracy requires a multifaceted strategy, including:

* Vigorously enforcing current federal copyright laws against all forms of piracy;
* Using digital rights management technologies available in the market to protect content at the source wherever possible;
* Expediting availability of authorized video-on-demand services via the Internet so paying customers have some viable options;
* Educating consumers about the importance and value of intellectual property;
* Taking serious measures to secure the physical distribution chain for content and better protect the source of online copyrighted works.

ITI also supports efforts to facilitate and expedite the DTV transition, both because consumers will benefit from the performance and interactivity of digital technology and because the spectrum now occupied by analog television can be put to many beneficial uses when the DTV transition is complete and that spectrum is surrendered back to the public.

While ITI and its member companies have participated extensively in the Broadcast Protection Discussion Group and are interested in effective content protection, we continue to have significant reservations regarding numerous issues related to implementation of the broadcast flag or any similar DTV content protection system.

Digital broadcast copy protection.

The premise of this proceeding and the chief question posed in the NPRM is whether the absence of a digital broadcast copy protection system is causing content owners to withhold quality programming and thereby

hindering the digital transition. In that context, it is appropriate to examine the relevant incentives and disincentives for programmers and the likely effects that might follow if the Commission were to adopt the broadcast flag or a similar system.

Free vs. free - the nature of TV

Broadcast television is a unique distribution channel for content protection purposes because the TV programs are distributed to the general public, unprotected and free of charge. This is relevant because, by definition, the content that might be pirated at a later date has already been made available to anyone with an antenna - which would presumably have a deleterious effect on the market for pirated works.

The unique danger cited by broadcasters is not that consumers might be able to watch TV programs without paying, or even that the viewer might make a personal copy without authorization. Those things are not only legal, they are expected. The apparent danger to future profits in the context of DTV are that such programming might be archived in a network available to the general public and that the downstream value of television shows on broadcast networks might be diminished if consumers preferred to download a TV show from the Internet instead of watching a syndicated rerun - or that consumers who did not tape a movie when it ran on broadcast might be able to find it later online instead of buying or renting it.

To genuinely deter content owners' embrace of DTV, the danger of piracy must diminish the market for later uses of TV programs. In effect, the download experience must create a substantial competitor to the rerun experience (both of which are free to the consumer) or the resale of old TV shows.

Evolution of sophisticated "time shifting."

The download vs. rerun issue must also be examined in the context of potential changes in the way people may watch television in the future, such as the proliferation of sophisticated personal video recorders (like TiVo and ReplayTV) that can scan the 100 channels offered by cable and satellite and collect the viewer's favorite programs to be watched at a time of his choosing.

Will the temptation to download your favorite "Seinfeld" episode be as great when your PVR has been accumulating "Seinfelds" as they appear every weekday evening for the past year? If personal video recorders begin to simulate the video-on-demand experience by perfectly legal means, any threat from the Internet to broadcast television will be further diminished. Of course not everyone has personal video recorders, but the likelihood of having such technology is substantially greater among households with the broadband Internet connection to download television shows and the DTV monitor to view them.

For a feature movie to have its downstream markets impacted by running on broadcast television, it must have been kept secure and out of the unauthorized peer-to-peer networks throughout all its previous distribution channels, such as theatrical release, pay-per-view, premium cable, sales and rental - all of which typically occur before a feature

film appears on free broadcast television. This is particularly difficult in the current environment where, according to congressional testimony, first-run movies are frequently compromised in the pre-release phase and available on peer-to-peer networks before they run in theaters. Copy protection features applied at the end of a movies' release life might be a several years too late.

The threshold of effectiveness for digital broadcast copy protection.

The other half of the equation is that the copy protection measures contemplated must be sufficiently robust to boost content owners' confidence to make their quality programming available via digital broadcast. The most effective means of protection would be encryption of digital broadcasts at the source, as has been done with cable, satellite, DVD and Internet video-on-demand services. While no technological copy protection system can be fool proof against a determined elite hacker, end-to-end encryption systems have proven effective at preventing piracy at the hands of average consumers and casual users. Throughout the Broadcast Protection Discussion Group process and in private inter-industry talks, the information technology industry has consistently pointed out that encrypting digital broadcasts at the source would be the most effective way to protect such content.

By contrast, the broadcast flag approach envisions transmitting such signals in the clear (unencrypted) with a "flag" attached to each television show indicating the content owner's wish to prohibit redistribution beyond certain parameters. Televisions, set-top boxes and computers that contained DTV receivers would presumably be required to read the flag and ensure against impermissible redistribution thereafter.

Unfortunately, no matter how secure a machine keeps the signal after it has demodulated it, the decision not to encrypt on the front end puts a serious handicap on the level of security that can ever be attained with the flag approach. If the broadcast flag were implemented, all DTV receivers with digital outputs, (such as tuner cards) manufactured before its implementation would become an instant "hole" in the system because they would not be programmed to read for the flag. This is significant because the apparent concern of broadcasters is not the individual consumers who make personal copies of broadcast content for themselves, but rather those who redistribute such content or make it available to unauthorized peer-to-peer networks and similar sources on the Internet. Thus, a small number of users redistributing the content would presumably do the requisite amount of damage to cause programmers to withhold their quality content after all.

Legacy equipment notwithstanding, the fact that such content was available unencrypted over the airwaves would create a permanent weak spot in the distribution chain that pirates could exploit without even the trouble of cracking encryption. As computing power increased over time, the ease of using software demodulators or other technology that ignored the flag would increase and broadcasters would have no way of evening the score (as they would with modulated encryption). Once the "demodulation hole" reached critical mass, broadcasters would have to either start encrypting their transmissions after all or face the loss of confidence (and quality programming) by content providers. Unfortunately, starting to encrypt at such a late date would mean

thousands of additional legacy receivers in the market that would have to be tracked down and outfitted with decryption converter boxes.

The danger of political obstacles to DTV.

Establishing the existence of an actual disincentive to offer quality programming AND the existence of a viable content protection scheme are both critical threshold questions for the Commission to answer. If the answer is negative on either count, there is a significant danger of creating a false political obstacle to the DTV transition and adding yet another item to the list of issues to be solved before programmers are expected to make their best content available. The danger would be compounded by demands that would inevitably arise for additional solutions (and regulations) to compensate for the inadequacies in the broadcast flag solution - drawing the Commission ever deeper into a regulatory regime to prop up its chosen approach.

Innovation, gatekeepers, objective criteria and self-certification.

If the Commission did proceed with a broadcast flag or similar regulation, it would face many of the hard choices that industry encountered in the BPDG process. As the NPRM points out, BPDG participants agreed that a broadcast flag system was possible but failed to reach complete agreement on some significant points of the compliance and robustness rules that would be associated with the flag to ensure that its proscriptions were honored by the equipment. The core of disagreement was a demand by the entertainment industry for specific assurances that each device would keep the signal secure and ensure that the signal was only shared with other similarly secure devices - and the resistance of technology companies to either highly specific design rules, a subjective process that gave another industry veto power over new components, or a bottleneck for government approval of new technologies. Private sector participants found no mutually agreeable means of addressing this conundrum, even if government action was assumed.

Any regime for approval of new output technologies must offer as one option, technical and licensing-based functional criteria to which technology companies could self-certify their compliance.

Robust security and the weakest link.

The inherent security limits of a flag-based copy protection system should also play a crucial role in any decisions about downstream devices, outputs and robustness of receiving devices. To wit, every incremental increase in robustness requirements for devices passes costs onto the consumer, but increasing security beyond the level offered at the first link in the chain (where the content is broadcast in the clear) yields no additional security benefits because pirates already have a weaker link to attack which can never be strengthened unless the broadcasts are ultimately encrypted. So for example, the entertainment and technology industries disagreed over the level of skill and tools of the hacker that the robustness rules should be designed to repel - but the fact that the signal is in the clear at the front end should obviate the need for a higher standard of security at the back end.

Consumer expectations and the scope of the flag

BPDG participants never agreed on the scope of use restrictions that the flag should signify. Should the system prevent all unauthorized redistribution? Should it define a "personal digital network environment" and limit distribution to that network? Some parties have advocated a broadcast flag that limited consumers to authorized activities and those that were widely considered to be fair use. Others wanted to be certain that no legitimate consumer expectation would be curtailed by the broadcast flag scheme.

If the Commission chose to mandate a broadcast flag, ITI would urge it to prevent only those activities that substantially endangered later commercial exploitation of TV programs. In other words, only keep it away from the kinds of publicly available archive Internet sites or unauthorized peer-to-peer networks that might offer a viable alternative to flipping through the dial or checking for favorites on the TiVo player.

Any effort to provide a more elaborate content protection scheme would inevitably put the Commission in the role of regulating copyright protections and making judgments about what was and wasn't fair use under the law. This would be especially true if the mandated copy protection technologies restricted any activities that were arguably fair use, because the Commission would be supplanting decades of federal copyright jurisprudence with its own judgments about what activities consumers should be allowed to engage in without specific authorization from copyright owners. The only way to avoid such a conundrum would be to intentionally give wide berth to consumer expectations and make no pretense of hewing to the contours of allowable copyright activities.

## Conclusion

ITI and its member companies continue to make ourselves available for inter-industry discussions with broadcasters, content owners, consumer electronics companies, consumer groups and all interested stakeholders on the difficult questions of how to protect digital content in broadcast television and in all the other channels. We firmly believe that there is no "silver bullet" to stop digital piracy, but that it is worthwhile to pursue a range of measures, including vigorous enforcement of existing anti-piracy laws - many of which were passed with the assistance of the information technology industry to address software piracy.

While sales for DVDs and other "aftermarket" goods normally impacted by piracy are booming at the moment, we recognize that piracy is a significant issue and could present a substantial danger in the future if left unchecked and we have committed hundreds of millions of dollars to address it. The ultimate solution for DTV could lie in encrypting the content, in finding an effective and mutually agreeable "flag" regime, or in reducing end user piracy by completely different means - and we are engaged on all fronts. We look forward to the continuing dialogue.

Respectfully submitted,
INFORMATION TECHNOLOGY INDUSTRY COUNCIL

By _____/s/_____

Rhett Dawson
President

December 6, 2002